Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

О НЕКОТОРЫХ НОРМАТИВНО-ПРАВОВЫХ КОЛЛИЗИЯХ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ ЭЛЕКТРОСВЯЗИ

В.А. БОЙПРАВ, Л.Л. УТИН

Белорусский государственный университет информатики и радиоэлектроники

В последние годы наблюдается определенная тенденция по увеличению удельного веса организаций, использующих в своей деятельности сети электросвязи для получения и предоставления информации, а также обмена сообщениями. При этом в большинстве случаев их эффективность функционирования и объемы прибыли зависят от качества и полноты выполнения организациями электросвязи своих обязанностей, определенных в Законе Республики Беларусь от 19 июня 2005 года № 45-З «Об электросвязи».

Деятельность организаций электросвязи сопряжена с созданием, эксплуатацией и обслуживанием критически важных объектов информатизации (КВОИ), нарушение функционирования которых может привести к негативным последствиям в информационной и экономической сферах национальной безопасности. В связи с этим одними из составляющих системы менеджмента защиты информации организаций электросвязи являются процедуры по внутреннему и внешнему контролю их КВОИ, регламентированному Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» и приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30 апреля 2012 г. № 42 «Об утверждении Инструкции о порядке проведения внешнего контроля за обеспечением безопасности критически важных объектов информатизации» [1, 2].

В работе [3] показано, что в действующих нормативных технических правовых актах, регламентирующих вопросы аудита системы менеджмента защиты информации в организациях электросвязи, не представлены однозначные определения и термины, которыми следует оперировать при реализации названного процесса. Зачастую это приводит к возникновению коллизий в правовой области. Несмотря на существующие проблемы в вопросе терминологии, можно говорить об однозначности определений, следующих основных регламентированных терминов.

1. Защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности, сохранности и других свойств информации.

2. Безопасность информации (или информационная безопасность) – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность, доступность и другие свойства информации при ее обработке техническими средствами.

3. Система менеджмента защиты информации – обязательная составляющая системы менеджмента организации электросвязи, включающая в себя политики, процедуры, рекомендации и связанные с ними человеческие ресурсы, инфраструктуру и производственную среду, целью которых являются создание, внедрение, функционирование, мониторинг, анализ, поддержка и улучшение системы защиты информации организации.

Таким образом, аудит системы менеджмента защиты информации является составляющей аудита системы менеджмента организации в целом.

Кроме того, из-за недостаточной проработки вопросов, регламентирующих особенности использования КВОИ организациями электросвязи различных категорий, создаются

предпосылки нецелевого использования средств, выделяемых для обеспечения качества функционирования созданных систем информационной безопасности.

В целях разрешения указанного выше противоречия предлагается разделять организации электросвязи на следующие категории (в зависимости от специфики деятельности этих организаций):

1 – организации, занимающиеся строительством сетей и сооружений электросвязи;

2 – организации, занимающиеся предоставлением услуг электросвязи;

3 – организации, занимающиеся проектированием сетей и сооружений электросвязи;

4 – организации, являющиеся органами, осуществляющими государственное регулирование и управление в области электросвязи.

Наиболее сложная ситуация сложилась на рынке услуг по строительству сетей, систем и сооружений электросвязи. После отмены лицензий на осуществление этого вида деятельности количество организаций, занимающихся строительством сетей и сооружений электросвязи, начало расти.

Значительная часть этих организаций осуществляла строительство промышленных и жилых объектов, но сокращение финансирования этого сектора экономики вынуждает их изменять направление своей деятельности.

Возросшая конкуренция на рынке строительства объектов электросвязи способствовала снижению стоимости выполняемых работ, при одновременном повышении уязвимости КВОИ и всех сетей электросвязи в целом. Принцип отбора подрядных организаций на выполнение работ по строительству объектов электросвязи не включает требований по наличию собственной системы менеджмента защиты информации и не предусматривает проведение проверки эффективности ее функционирования. Мелкие и средние строительные компании постоянно прибегают к практике приема на работу специалистов, набранных по рекламным объявлениям, для реализации конкретных объектов. Настоящая практика приводит к бесконтрольному допуску большого количество случайных людей на КВОИ и дает возможность вмешаться в процесс их функционирования или вывести из эксплуатации.

Следовательно, с учетом стремительного роста количества подрядных строительных организаций, отсутствия регулирования их деятельности на сетях электросвязи, а также с точки зрения количества потенциальных уязвимостей КВОИ, доступ к которым имеют сотрудники этих организаций, предлагается последние отнести к 1 категории.

Увеличение организаций, получивших лицензии на предоставление услуг электросвязи и имеющаяся у большинства из них возможность подключиться к телефонным сетям общего пользования, создают угрозу нарушения работоспособности КВОИ. Количество этих организаций и количество используемых классов КВОИ позволяет отнести их ко 2 категории организаций с точки количества уязвимостей КВОИ.

Организации, занимающиеся проектированием сетей, систем и сооружений связи можно отнести к 3 категории организаций с точки зрения количества КВОИ, доступ к которым имеют их сотрудники, по причине ограниченности прямого доступа на КВОИ и сетям электросвязи.

Органы государственного управления, занимающиеся регулированием в области электросвязи, отнесены к 4 категории из-за высокой квалификации персонала и наличия в их структуре специалистов по спецработе.

Таким образом, категорирование организаций электросвязи будет способствовать снижению временных затрат на проведение аудита их системы менеджмента защиты информации как совокупности мероприятий, направленных не на оценку состояния защи-

щенности информации, а на оценку качества реализации процессов, связанных с созданием, внедрением и функционированием системы защиты информации организации. Снижение временных затрат на проведение аудита связано со следующими причинами, обуславливающими уменьшение количества нормативных и правовых коллизий при реализации названного процесса: корректный выбор круга лиц из числа сотрудников аудируемой организации; точное определение перечня анкетных вопросов для сотрудников аудируемой организации; корректные планирование и определение очередности проведения аудита системы менеджмента защиты информации в организациях электросвязи (в случае выполнения задачи по проведению аудита в нескольких организациях одновременно).

Список литературы

1. О некоторых мерах по обеспечению безопасности критически важных объектов информатизации : Указ Президента Респ. Беларусь, 25 окт. 2011 г., № 486 // Нац. реестр правовых актов Респ. Беларусь. – 2011. – № 121. – 1/13026.

2. Об утверждении Инструкции о порядке проведения внешнего контроля за обеспечением безопасности критически важных объектов информатизации : Приказ Оперативно-аналитического центра при Президенте Респ. Беларусь 30 апр. 2012 г., № 42 // Нац. реестр правовых актов Респ. Беларусь. – 2012. – № 52. – 7/2003.

3. Бойправ, В.А. Принципы реализации методики аудита системы менеджмента защиты информации в организациях электросвязи / В.А. Бойправ, Л.Л. Утин // Доклады БГУИР. – 2016. – № 6 (100). – С. 94–99.

НОРМАТИВНО-ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ РЕСПУБЛИКИ БЕЛАРУСЬ

А.В. ДЕНИСЕВИЧ

Оперативно-аналитический центр при Президенте Республики Беларусь

В настоящее время по оценке Международного союза электросвязи Республика Беларусь по итоговому индексу развития информационно-коммуникационных технологий поднялась с 52 места в 2011 г. на 31-е в 2016 г. среди 175 стран. За данный период в Беларуси создан базовый комплекс электронного правительства, в который входят такие компоненты как: общегосударственная автоматизированная информационная система, система межведомственного электронного документооборота, Государственная система управления открытыми ключами проверки электронной цифровой подписи, единое расчетное информационное пространство. Завершено строительство Республиканского центра обработки данных. Осуществляется информатизация здравоохранения, образования, социально-трудовой сферы. Основной задачей внедрения ИКТ в реальном секторе экономики является повышения эффективности управления полным циклом производства, создание интегрированных информационных систем, осуществляющих управление ресурсами предприятия. Развитие информатизации в Республике Беларусь приведет к появлению новых угроз национальной безопасности в информационной сфере, с которыми уже столкнулись страны с высоким индексом развития ИКТ. Объекты в отношении которых могут быть реализова-